Listing of Claims

1. (Original) A method of transferring network security based communications from a first distribution processor, which provides secure communications over a network in a distributed workload environment having target hosts which are accessed through the first distribution processor by a common network address, to a second distribution processor, the method comprising:

providing information sufficient to restart the transferred network security based communications at the second distribution processor;

detecting takeover of the common address by the second distribution processor;

terminating existing network security based communications to the first distribution processor;

restarting the transferred network security based communications at the second distribution processor utilizing the provided information;

routing both inbound and outbound network security based communications with target hosts utilizing the common network address through the second distribution processor; and

network security processing both the inbound and the outbound network security based communications utilizing the common network address at the second distribution processor.

2. (Original) A method according to Claim 1, further comprising the step of identifying transferred network security based communications local to the first distribution processor utilizing the common network address as distributed communications so as to cause communications utilizing the common network address and network security to be routed through the second distribution processor.

3. (Original) A method according to Claim 1, wherein the step of providing information sufficient to restart communications comprises the step of transmitting, from the first distribution processor to the second distribution processor prior to termination of the existing secure communications to the first distribution processor, network security information from which network security relationships associated with the transferred network security based

communications through the first distribution processor can be re-established at the second distribution processor.

4. (Original) A method according to Claim 1, wherein the step of providing information sufficient to restart communications comprises the step of storing in a common storage accessible to the second distribution processor, network security information from which network security relationships associated with the transferred network security based communications through the first distribution processor can be re-established at the second distribution processor.

5. (Original) A method according to Claim 4, wherein the step of restarting the transferred network security based communications at the second distribution processor utilizing the provided information, comprises the following steps carried out by the second distribution processor:

obtaining the network security information from the common storage;

establishing the security relationships associated with the transferred network security based communications through the first distribution processor at the second distribution processor; and

notifying target hosts associated with the transferred network security based communications that the second distribution processor has taken ownership of the transferred network security based communications.

6. (Original) A method according to Claim 5, further comprising the step of clearing the network security information from the common storage subsequent to the second distribution processor obtaining the network security information from the common storage.

7. (Original) A method according to Claim 5, further comprising the step of placing in the common storage, network security information from which network security relationships associated with network security based communications through the second distribution processor can be re-established at another distribution processor.

8. (Original) A method according to Claim 5, further comprising the step of identifying as non-distributed communications, ones of the transferred network security based communications local to the second distribution processor which were previously distributed communications routed through the first distribution processor.

9. (Original) A method according to Claim 5, wherein the network security comprises Internet Protocol Security (IPSec).

10. (Original) A method according to Claim 9, wherein the information stored in the common storage comprises at least one of Phase 1 Security Association (SA) information, Phase 2 SA information and information relating the Phase 1 SA information to the Phase 2 SA information.

11. (Original) A method of transferring Internet Protocol Security (IPSec) communications from a first routing communication protocol stack to a second routing communication protocol stack, wherein the first routing communication protocol stack routes the IPSec communications from a network to a plurality of application instances executing on a cluster of data processing systems utilizing a virtual Internet Protocol Address (VIPA) Distributor and which distributes the IPSec communications for connections to at least one dynamically routable VIPA (DVIPA) to a plurality of target communication protocol stacks, the method comprising the steps of:

detecting takeover of the at least one DVIPA by the second routing communication protocol stack;

reading IPSec information for IPSec security associations (SAs) associated with the at least one DVIPA from a coupling facility of the cluster of data processing systems;

deleting the IPSec SAs associated with the at least one DVIPA at the first routing communication protocol stack;

renegotiating the IPSec SAs between the second routing communication protocol stack and remote IPSec peers utilizing the at least one DVIPA based on the IPSec information read from the coupling facility;

re-routing the connections to the at least one DVIPA through the second routing communication protocol stack; and

performing IPSec processing for the re-routed connections to the at least one DVIPA at the second routing communication protocol stack utilizing the renegotiated IPSec SAs.

12. (Original) A method according to Claim 11, further comprising the step of preventing the first routing communication protocol stack from placing new information associated with the at least one DVIPA in the coupling facility.

13. (Original) A method according to Claim 11, further comprising the step of identifying connections to the at least one DVIPA which are local to the first routing communication protocol stack as distributed so as to route such communications through the second communication protocol stack.

14. (Original) A method according to Claim 11, wherein the step of renegotiating the IPSec SAs comprises the steps of:

notifying an instance of an Internet Key Exchange (IKE) application associated with the second routing communication protocol stack of the takeover of the at least one DVIPA from the first routing communication protocol stack;

providing the read IPSec information to the IKE application;

negotiating new IPSec SAs associated with the at least one DVIPA utilizing the IKE application; and

installing the new IPSec SAs in the second routing communication protocol stack.

15. (Original) A method according to Claim 14, wherein the IPSec SAs comprise Phase 1 SAs and Phase 2 SAs, the method further comprising steps of:

storing new Phase 1 SA information in the coupling facility; and

storing new Phase 2 SA information in the coupling facility.

16. (Original) A method according to Claim 11, further comprising the step of clearing the IPSec information from the coupling facility after the IPSec information is read from the coupling facility.

17. (Original) A method according to Claim 11, wherein the first routing communication protocol stack carries out the steps of:

establishing IPSec SAs with remote IPSec peers utilizing the at least one DVIPA; and

storing IPSec SA information in the coupling facility sufficient to allow renegotiation of the established IPSec SAs.

18. (Original) A method according to Claim 11, wherein the IPSec SA information comprises at least one of cached Phase 1 SA policies, Phase 1 SA identifications, information correlating Phase 1 SAs and Phase 2 SAs, dynamic filter selectors and cryptographic policies.

19. (Original) A method according to Claim 18, wherein the IPSec SA information further comprises IPSec Security Parameter Indexes (SPIs) and protocols for the Phase 2 SAs, the method further comprising the steps of:

installing IPSec dynamic filters in the second routing communication protocol stack;

removing duplicates of active dynamic filters; and

sending a delete to an IKE associated with the first routing communication protocol stack for IPSec SAs that were active on the first routing communication protocol stack.

20. (Original) A system for transferring network security based communications from a first distribution processor, which provides secure communications over a network in a distributed workload environment having target hosts which are accessed through the first distribution processor by a common network address, to a second distribution processor, comprising:

means for providing information sufficient to restart the transferred network security based communications at the second distribution processor;

means for detecting takeover of the common address by the second distribution processor;

means for terminating existing network security based communications to the first distribution processor;

means for restarting the transferred network security based communications at the second distribution processor utilizing the provided information;

means for routing both inbound and outbound network security based communications with target hosts utilizing the common network address through the second distribution processor; and

means for network security processing both the inbound and the outbound network security based communications utilizing the common network address at the second distribution processor.

21. (Original) A system for transferring Internet Protocol Security (IPSec) communications from a first routing communication protocol stack to a second routing communication protocol stack, wherein the first routing communication protocol stack routes the IPSec communications from a network to a plurality of application instances executing on a cluster of data processing systems utilizing a virtual Internet Protocol Address (VIPA) Distributor and which distributes the IPSec communications for connections to at least one dynamically routable VIPA (DVIPA) to a plurality of target communication protocol stacks, comprising:

means for detecting takeover of the at least one DVIPA by the second routing communication protocol stack;

means for reading IPSec information for IPSec security associations (SAs) associated with the at least one DVIPA from a coupling facility of the cluster of data processing systems;

means for deleting the IPSec SAs associated with the at least one DVIPA at the first routing communication protocol stack;

means for renegotiating the IPSec SAs between the second routing communication protocol stack and remote IPSec peers utilizing the at least one DVIPA based on the IPSec information read from the coupling facility;

means for re-routing the connections to the at least one DVIPA through the second routing communication protocol stack; and

means for performing IPSec processing for the re-routed connections to the at least one DVIPA at the second routing communication protocol stack utilizing the renegotiated IPSec SAs.

22. (Original) A computer program product for transferring network security based communications from a first distribution processor, which provides secure communications over a network in a distributed workload environment having target hosts which are accessed through the first distribution processor by a common network address, to a second distribution processor, comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which provides information sufficient to restart the transferred network security based communications at the second distribution processor;

computer readable program code which detects takeover of the common address by the second distribution processor;

computer readable program code which terminates existing network security based communications to the first distribution processor;

computer readable program code which restarts the transferred network security based communications at the second distribution processor utilizing the provided information;

computer readable program code which routes both inbound and outbound network security based communications with target hosts utilizing the common network address through the second distribution processor; and

computer readable program code which network security processes both the inbound and the outbound network security based communications utilizing the common network address at the second distribution processor.

23. (Original) A computer program product for transferring Internet Protocol Security (IPSec) communications from a first routing communication protocol stack to a second routing communication protocol stack, wherein the first routing communication protocol stack routes the IPSec communications from a network to a plurality of application instances executing on a cluster of data processing systems utilizing a virtual Internet Protocol Address (VIPA) Distributor and which distributes the IPSec communications for connections to at least one dynamically routable VIPA (DVIPA) to a plurality of target communication protocol stacks, comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which detects takeover of the at least one DVIPA by the second routing communication protocol stack;

computer readable program code which reads IPSec information for IPSec security associations (SAs) associated with the at least one DVIPA from a coupling facility of the cluster of data processing systems;

computer readable program code which deletes the IPSec SAs associated with the at least one DVIPA at the first routing communication protocol stack;

computer readable program code which renegotiates the IPSec SAs between the second routing communication protocol stack and remote IPSec peers utilizing the at least one DVIPA based on the IPSec information read from the coupling facility;

computer readable program code which reroutes the connections to the at least one DVIPA through the second routing communication protocol stack; and

computer readable program code which performs IPSec processing for the re-routed connections to the at least one DVIPA at the second routing communication protocol stack utilizing the renegotiated IPSec SAs.